30 October 2026

To whom it may concern,

iBeta Quality Assurance conducted Presentation Attack Detection (PAD) testing in accordance with ISO/IEC 30107-3. iBeta is accredited by NIST/NVLAP (NVLAP Testing Lab Code: 200962) to test and provide results to this PAD standard (certificate and scope may be downloaded from the NVLAP website).

This testing was conducted with MSC Trustgate.com Sdn. Bhd.'s MyTrust MobileID eKYC Client v2.2.2 application installed on a Samsung Galaxy S25 running Android 16 and an Apple iPhone 17 running iOS 26.0.1, supported by backend server component MyTrust MobileID eKYC Server v1.3.2. iBeta conducted active liveness detection testing from 6 October to 30 October 2026.

Testing was conducted in accordance with the contract for a level of spoofing technique that only utilized simple, readily available methods to create artefacts of the genuine biometric for use in the presentation attack. The subjects for the test effort were cooperative – meaning that they were willing and able to provide any and all biometric samples, including high-quality facial images. The test time for each PAD test per PAI was limited to eight hours. This is considered a Level 1 PAD test effort (first of three levels).

The test method involved enrolling subjects and having them authenticate five times successfully. Six species of presentation attacks (PAs) were then attempted ten times each. Results appeared on each device as "true" for a successful attempt and "false" for an unsuccessful attempt; a failure to acquire the PA three times for 30 seconds per attempt was also considered unsuccessful. A total of 720 presentation attacks (360 per device) were attempted. At the conclusion of the PAD testing, the subject returned and authenticated five times successfully to verify that the application was still able to recognize the genuine subject.

iBeta was not able to gain unauthorized access with the PAs on either the Galaxy S25 or iPhone 17, yielding an overall Presentation Attack (PA) success rate of 0%, which then equates to the overall combined Imposter Attack Presentation Accept Rate (IAPAR) of 0%. The bona fide False Non-Match Rate (FNMR) was also calculated and may be found in the final report.

MSC Trustgate.com Sdn. Bhd.'s MyTrust MobileID eKYC Client v2.2.2 application and its backend server component MyTrust MobileID eKYC Server v1.3.2 were tested by iBeta as a biometric facial recognition system to the ISO 30107-3 Biometric Presentation Attack Detection Standard and were found to be in compliance with Level 1.

Best regards,



Ryan Borgstrom
iBeta Quality Assurance Director of Biometrics
rborgstrom@ibeta.com
303.627.1110 extension 182